

UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with Facebook User ID  
100004598130172, that is stored at premises controlled by  
Facebook

)  
)  
)  
)  
)  
)

Case No. 19-MJ-1363

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

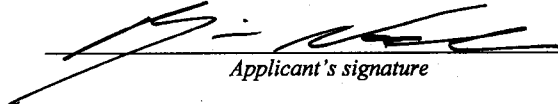
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Section 3148.

The application is based on these facts: See attached affidavit.

- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Brian Nodes, Deputy Marshal, U.S. Marshals Service  
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 12/6/19

  
Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Brian Nodes, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook User ID that is stored at premises owned, maintained, controlled, or operated by Facebook, Inc. ("Facebook"), a social networking company headquartered at 1601 Willow Road, Menlo Park, California 94025. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the User ID.

2. I am employed as a Deputy with the United States Marshals Service and have held that position for approximately 10 years. As part of my duties, I conduct investigations to locate federal and state fugitives.

3. In December 2008, I completed a 12-week training course at the Federal Law Enforcement Training Center located in Glynco, Georgia. In March 2009, I also completed the Basic Deputy Course, a six-week course at the U.S. Marshals Service Training Academy located in Glynco, Georgia. I have had both formal training and have participated in several investigations that utilize various electronic surveillance techniques. These techniques have proven to be useful in locating individuals who are actively avoiding arrest.

4. I am an investigator or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 3148, have been committed by Julion S. Griffin, also known as Jewel D. Griffin. This affidavit is made in support of an application for a search warrant to search the Target Account, more fully described in Attachment A, for evidence and instrumentalities, more fully described in Attachment B, for violations of Title 18, United States Code, Section 3148. I am seeking historical and real-time location information for the Target Account from Facebook, Inc. There is also probable cause to search the information described in Attachment A for evidence of these crimes and the whereabouts of a person to be arrested, as described in Attachment B.

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated pursuant to 18 U.S.C. § 2711(3)(A)(i).

## FACEBOOK TECHNICAL BACKGROUND

8. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

9. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

10. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

11. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A

Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook. Depending on the user's privacy settings, Facebook may also obtain and store the physical location of the user's device(s) as they interact with the Facebook service on those device(s).

12. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

13. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.



14. Facebook users can exchange private messages on Facebook with other users.

Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

15. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

16. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

17. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

18. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

19. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

20. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page:

21. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so. Based on my training and experience, I know that Facebook can provide real-time location history of a Facebook account, including the date and time associated with a latitude and longitude.

22. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

23. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s

profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

24. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account and the whereabouts of that person. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under



investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

25. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications and real-time location information) particularly described in Section I of Attachment B. Upon receipt of the information described in Sections I and II of Attachment B, government-authorized persons will review that information to locate the items described in Section III of Attachment B.

### **PROBABLE CAUSE**

27. I am involved in a criminal investigation of a violation of the conditions of supervised release, in violation of Title 18, United States Code, Section 3148. On or about July 9, 2019, an indictment was filed against Julion S. Griffin, also known as Jewel D. Griffin—the subscriber of the Target Account—in Case No. 19-CR-124. In that indictment, the Grand Jury charged the defendant with violations of Title 18, United States Code, Sections 922(g)(1) and 924(a)(2).

28. The defendant was arrested on an arrest warrant and arraigned on July 29, 2019. The defendant was temporarily detained. On July 31, 2019, the Court released the defendant with conditions pending trial, over the objection of the United States. Those conditions required the defendant to appear in court as required, advise the court or pretrial services office or supervising officer in writing before making any change of residence or telephone number, submit to supervision by and report for supervision to the pretrial services office as directed, and submit to location monitoring as directed by the pretrial services office or supervising officer. In that order, the defendant was advised of the penalties for violating the conditions of release and signed an acknowledgment to that effect on July 30, 2019.

29. On October 10, 2019, the defendant advised the pretrial service officer of a residence change, but never provided an address. Later that day, the pretrial service officer received an alert that the defendant had cut off his location monitoring device. In response, the pretrial services officer attempted to contact the defendant multiple times with no response.

30. The United States District Court for the Eastern District of Wisconsin issued an arrest warrant for the defendant as a result of a violation of his release conditions on October 11, 2019.

31. The United States Marshals Service has been enlisted to locate and apprehend the defendant. As of today, the defendant's whereabouts remain unknown, and the arrest warrant remains unexecuted.

32. I received information from the pretrial service officer that Julion S. Griffin (DOB: 12/29/1990) uses an alias of Jewel D. Griffin, as reflected in the indictment. The U.S. Marshals Service conducted a reference check on the defendant, which included comparing Julion Griffin's booking photograph to the Wisconsin Department of Transportation's driver's license photograph of Jewel D. Griffin.

33. I have conducted surveillance of locations associated with the defendant. On December 5, 2019, the U.S. Marshals Great Lakes Regional Fugitive Task Force in Milwaukee conducted a surveillance operation for the defendant. During the investigation, I learned that the defendant had a relationship with Kayla Smith (DOB: 09/04/1995) and identified a black 2009 Audi A6 bearing Wisconsin license plate AHE-7095 that was registered to her at 5270 North 91<sup>st</sup> Street, Unit 7 in Milwaukee, Wisconsin.

34. On December 5, 2019, U.S. Marshals located that vehicle parked in a driveway in the vicinity of 101-107 West Meinecke Avenue in Milwaukee. Investigators later observed Griffin approaching the vehicle, open the driver's side door, and then reverse the vehicle into the street. Investigators approached the defendant, activated emergency lights and sirens, and attempted to conduct a positive vehicle containment, a law enforcement technique to stop and contain a vehicle in an effort to avoid a vehicle pursuit.

35. Investigators made vehicle contact with the passenger door side of Griffin's vehicle, while two other law enforcement vehicles approached from the driver's side. Upon observing the law enforcement vehicles, the defendant placed his vehicle into drive and drove forward, breaking containment from law enforcement. The defendant then fled at a high rate of speed westbound on Meinecke Avenue. Investigators continued to follow the defendant with emergency lights and sirens activated. The defendant did not stop, but instead led investigators on a high-speed pursuit. Investigators continued for approximately 0.8 miles before terminating the pursuit. During that pursuit, the defendant disregarded four stop signs and reached speeds between 80 and 100 miles per hour.

36. I conducted an open records search on Facebook by typing in the name Jewel Griffin and located Facebook profile "Jewel Dominique Griffin" (URL: [https://www.facebook.com/jdbackagain\\_with\\_associated](https://www.facebook.com/jdbackagain_with_associated); User ID 100004598130172). This profile is available for public viewing. I compared the photographs on this Facebook profile, the driver's license photograph of Jewel D. Griffin, and booking photograph of Julion S. Griffin, also known as Jewel D. Griffin, and found that the photographs matched.

37. On November 20, 2019, I submitted a preservation request to Facebook, Inc.

38. Based on my training and experience in locating and apprehending potentially violent fugitives, the requested information will assist in locating the defendant. This information will provide information about his associates, his historical location, and his real-time location.

39. Because successful apprehensions, particularly of violent fugitives, often rely on the element of surprise, it is often necessary to attempt an arrest during nighttime or the early morning hours, when most people are sleeping. Further, apprehension tactical plans often change

at the last minute based on unexpected movements or other behavior of the target. Therefore, I cannot predict in advance when the real-time data would need to be accessed, and would need access to the real-time data at all times of the day or night in order to ensure a safe and successful apprehension.

#### **CONCLUSION**

40. Based on the forgoing, I request that the Court issue the proposed search warrant.



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the Facebook user ID 100004598130172 and associated Facebook account <https://www.facebook.com/jdbackagain> that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered 1601 Willow Road, Menlo Park, California 94025.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Historical information to be disclosed by Facebook, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities October 1, 2019 to December 5, 2019;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them October 1, 2019 to December 5, 2019, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification

numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (f) All other records and contents of communications and messages made or received by the user October 1, 2019 to December 5, 2019, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;
- (g) All "check ins" and other location information;
- (h) All IP logs, including all records of the IP addresses that logged into the account;
- (i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (j) All information about the Facebook pages that the account is or was a "fan" of;
- (k) All past and present lists of friends created by the account;
- (l) All records of Facebook searches performed by the account October 1, 2019 to December 5, 2019;
- (m) All information about the user's access and use of Facebook Marketplace;
- (n) The types of service utilized by the user;

- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (q) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within 7 days of service of this warrant.

**II. Real-time information to be disclosed by Facebook, Inc.**

- (a) All physical location data collected by Facebook for the user of the account, including any data collected by Facebook's location services via the user's mobile phone or other device, on a real-time or near-real time basis. Facebook is required to provide any such data they collect, regardless of the time of day.
- (b) All data disclosed by Facebook shall be made accessible by the provider to the United States Marshals Service at all times, day or night, and emailed to Deputy United States Marshal Brian Nodes at [Brian.Nodes@usdoj.gov](mailto:Brian.Nodes@usdoj.gov).
- (c) The provider shall begin producing the information required by this attachment within 7 days of the date of service of the warrant.
- (d) The provider shall produce the information required by this attachment for a period of 30 days from the date of issuance of this warrant.



### **III. Information to be seized by the government**

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Section 3148 involving Julion S. Griffin, also known as Jewel D. Griffin, since October 1, 2019, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Violations of the conditions of release;
- (b) The historical and current whereabouts of Julion S. Griffin, also known as Jewel D. Griffin;
- (c) Any and all associates of Julion S. Griffin, also known as Jewel D. Griffin;
- (d) Any other aliases for Julion S. Griffin, also known as Jewel D. Griffin;
- (e) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (f) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- (g) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Facebook, and my title is \_\_\_\_\_.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Facebook. The attached records consist of \_\_\_\_\_. I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Facebook, and they were made by Facebook as a regular practice; and
- b. such records were generated by Facebook's electronic process or system that produces an accurate result, to wit:
  1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Facebook in a manner to ensure that they are true duplicates of the original records; and
  2. the process or system is regularly verified by Facebook, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature